CLAIMS

1. A method for providing access between a first party and a second party, said method comprising the steps of:

generating a challenge value and a lock value at said first party;

transmitting said challenge to said second party;

generating a response value from said second party;

transmitting said response value to said first party; and

validating said response value by said first party.

2. The method of Claim 1, wherein said first party is a disk drive and said second party is a host computer.

3. The method of Claim 2, wherein said disk drive is locked when not accessed.

4. The method of Claim 3, wherein said step of generating a said challenge value and said lock value further includes the step of using 512 bits for said challenge value and using 512 bits for said lock value.

5. The method of Claim 4, wherein said step of generating a said challenge value and said lock value further includes the step of randomly generating each said challenge value.

6. The method of Claim 5, wherein said step of generating a said challenge value and said lock value further includes the step of using a disk drive controller to generate said challenge value.

7. The method of Claim 6, wherein said step of generating a said response value further includes the step of using an exclusive OR (XOR) to combine the said challenge and said lock values.

8. The method of Claim 7, wherein said step of generating a said response value further includes the step of using 160 bits for said response value.

9. The method of Claim 8, wherein said step of generating a said response value further includes the step of using a cryptography circuit to generate said response value.

10. The method of Claim 9, wherein said step of generating a said response value further includes the step of using an algorithm to generate said response value.

11. The method of Claim 10, wherein said step of generating a said response value further includes the step of using a secure hash algorithm to generate said response value.

12. The method of Claim 11, wherein said step of validating said response value further includes the step of said disk drive controller receiving the challenge and lock values, computing a duplicate response value by performing a duplicate said secure hash algorithm, and comparing the original said response value to the duplicate said response value.

13. The method of Claim 12, wherein said step of validating said response value further includes the step of unlocking the disk drive if the response and duplicate response values match.

14. An apparatus for providing access between a first party and a second party, said apparatus comprising:

means for generating a challenge value and a lock value at said first party;

means for transmitting said challenge to said second party;

means for generating a response value fat said second party;

means for transmitting said response value to said first party; and

means for validating said response value by said first party.

15. The apparatus of Claim 14, wherein said first party is a disk drive and said second party is a host computer.

16. The apparatus of Claim 15, wherein said disk drive is locked when not accessed.

17. The apparatus of Claim 16, wherein said means for generating a said challenge value and said lock value further includes using 512 bits for said challenge value and using 512 bits for said lock value.

18. The apparatus of Claim 17, wherein said means for generating a said challenge value and said lock value further includes means for randomly generating each said challenge value.

19. The apparatus of Claim 18, wherein said means for generating a said challenge value and said lock value further includes means for using a disk drive controller to generate said challenge value.

20. The apparatus of Claim 19, wherein said means for generating a said response value further includes an exclusive OR (XOR) for combining the said challenge and said lock values.

21. The apparatus of Claim 20, wherein said means for generating a said response value further includes using 160 bits for said response value.

22. The apparatus of Claim 21, wherein said means for generating a said response value further includes a cryptography circuit for generating said response value.

23. The apparatus of Claim 22, wherein said means for generating a said response value further includes an algorithm for generating said response value.

24. The apparatus of Claim 23, wherein said means for generating a said response value further includes a secure hash algorithm for generating said response value.

25. The apparatus of Claim 24, wherein said means for validating said response value further includes a means for said disk drive controller receiving challenge and lock values, computing a duplicate response value by performing a duplicate said secure hash algorithm, and comparing the original said response value to the duplicate said response value.

26. The apparatus of Claim 25, wherein said means for validating said response value further includes means for unlocking the disk drive if the response and duplicate response values match.